

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung

Columbia University, New York, NY, USA

More information about this subseries at <http://www.springer.com/series/7407>

Antonio Cerone · Peter Csaba Ölveczky (Eds.)

Theoretical Aspects of Computing – ICTAC 2021


18th International Colloquium

Virtual Event, Nur-Sultan, Kazakhstan, September 8–10, 2021

Proceedings

Editors

Antonio Cerone
Nazarbayev University
Nur-Sultan, Kazakhstan

Peter Csaba Ölveczky 
Department of Informatics
University of Oslo
Oslo, Norway

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-85314-3 ISBN 978-3-030-85315-0 (eBook)
<https://doi.org/10.1007/978-3-030-85315-0>

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer Nature Switzerland AG 2021

Chapter “Compositional Analysis of Protocol Equivalence in the Applied π -Calculus Using Quasi-open Bisimilarity” is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>). For further details see license information in the chapter.

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the proceedings of the 18th International Colloquium on Theoretical Aspects of Computing (ICTAC 2021), which was held during September 8–10, 2021. The event was supposed to take place in Nur-Sultan, Kazakhstan, but due to the pandemic it had to be held as a fully virtual event, organized by Nazarbayev University.

The conference concerns all aspects of theoretical computer science and aims at bringing together researchers and practitioners from academia, industry, and government to present research and exchange ideas and experience, addressing challenges in both theoretical aspects of computing and the exploitation of theory through methods and tools for system development. ICTAC also aims to promote research cooperation between developing and industrial countries.

ICTAC 2021 received 55 paper submissions. Almost all papers received at least three reviews. Based on the reviews and extensive discussions, the program committee decided to accept 20 papers. This volume contains the revised versions of these 20 papers, which cover a wide variety of topics, including: getting the best price for selling your personal data; attacking Bitcoin; optimizing various forms of model checking; synthesizing and learning algorithms; formalizing and verifying contracts, languages, and compilers; analyzing the correctness and complexity of programs and distributed systems; and finding connections from proofs in propositional logic to quantum programming languages.

The conference also featured invited talks by Wil van der Aalst (RWTH Aachen University, Germany), Alan Dix (Swansea University, UK), Kim Guldstrand Larsen (Aalborg University, Denmark), and Grigore Rosu (University of Illinois at Urbana-Champaign, USA). An abstract of the invited talk by Larsen and full papers accompanying those by van der Aalst and Dix are included in this volume.

Many colleagues and friends contributed to ICTAC 2021. We thank the invited speakers for accepting our invitations to give invited talks and the authors who submitted their work to ICTAC 2021. We are grateful to the members of the program committee and the external reviewers for providing timely and insightful reviews, as well as for their involvement in the post-reviewing discussions. We would also like to thank the regional publicity chairs for their work attracting submissions and Springer for sponsoring the Best Paper Award.

July 2021

Antonio Cerone
Peter Csaba Ölveczky

Organization

Program Chairs

Antonio Cerone
Peter Csaba Ölveczky

Nazarbayev University, Kazakhstan
University of Oslo, Norway

Steering Committee

Frank de Boer
Martin Leucker (Chair)
Zhiming Liu
Tobias Nipkow
Augusto Sampaio
Natarajan Shankar
Tarmo Uustalu

CWI, The Netherlands
University of Lübeck, Germany
Southwest University, China
Technical University of Munich, Germany
Federal University of Pernambuco, Brazil
SRI International, USA
Tallinn University of Technology, Estonia

Program Committee

Erika Ábrahám
Bernhard K. Aichernig
Musab A. Alturki

Étienne André
Ebru Aydin Gol
Kyungmin Bae

Maurice ter Beek
Dirk Beyer
Simon Bliudze
Roberto Bruni
Antonio Cerone
Manuel Clavel
Adrian Francalanza
Rob van Glabbeek
Sergey Goncharov

Jan Friso Groote
Stefan Gruner
Osman Hasan

Klaus Havelund
Kim G. Larsen

RWTH Aachen University, Germany
Graz University of Technology, Austria
Runtime Verification Inc., USA, and King Fahd
University of Petroleum and Minerals, Saudi Arabia
Université de Lorraine, France
Middle East Technical University, Turkey
Pohang University of Science and Technology,
South Korea
ISTI-CNR, Italy
Ludwig-Maximilian University Munich, Germany
Inria Lille, France
University of Pisa, Italy
Nazarbayev University, Kazakhstan
Vietnamese-German University, Vietnam
University of Malta, Malta
Data61, CSIRO, Australia
Friedrich-Alexander University Erlangen-Nürnberg,
Germany
Eindhoven University of Technology, The Netherlands
University of Pretoria, South Africa
National University of Sciences & Technology,
Pakistan
Jet Propulsion Laboratory, USA
Aalborg University, Denmark

Axel Legay	Université catholique de Louvain, Belgium
Martin Leucker	University of Lübeck, Germany
Manuel Mazzara	Innopolis University, Russia
Catherine Meadows	Naval Research Laboratory, USA
Larissa Meinicke	The University of Queensland, Australia
Hans de Nivelte	Nazarbayev University, Kazakhstan
Kazuhiro Ogata	JAIST, Japan
Peter Csaba Ölveczky	University of Oslo, Norway
Catuscia Palamidessi	Inria, France
Elaine Pimentel	Federal University of Rio Grande do Norte, Brazil
José Proença	Polytechnic Institute of Porto, Portugal
Riadh Robbana	INSAT, Carthage University, Tunisia
Gwen Salaün	University of Grenoble Alpes, France
Davide Sangiorgi	University of Bologna, Italy, and Inria, France
Lutz Schröder	Friedrich-Alexander University Erlangen-Nürnberg, Germany
Volker Stolz	Western Norway University of Applied Sciences, Norway
Georg Struth	The University of Sheffield, UK

Regional Publicity Chairs

Stefan Gruner	University of Pretoria, South Africa
Kazuhiro Ogata	JAIST, Japan
Elaine Pimentel	Federal University of Rio Grande do Norte, Brazil
Riadh Robbana	INSAT, Carthage University, Tunisia
Nikolay Shilov	Innopolis University, Russia

Additional Reviewers

Yehia Abd Alrahman	Karam Kharraz
Mario S. Alvim	Michalis Kokologiannakis
Tomer Ashur	Sandeep Kulkarni
Giorgio Bacci	Frédéric Lang
Marco Bernardo	Thomas Lemberger
Laura Bussi	Anders Miltner
Guillermina Cledou	Carlos Olarte
Khanh Huu The Dam	Renato Neves
Guillaume Dupont	Andrea Pferscher
Rick Erkens	Johannes Åman Pohjola
Lorenzo Gheri	Danny Bøgsted Poulsen
Imen Ben Hafaiedh	Adnan Rashid
Andreas Hülsing	Jose Ignacio Requeno
Peter Gjøl Jensen	Martin Sachenbacher

Wendelin Serwe
Francesco Sica
Flip van Spaendonck
Daniel Thoma

Adele Veschetti
Olivier Verdier
Nico Weise

Sponsor



NAZARBAYEV
UNIVERSITY

Model Checking and Machine Learning Joining Forces in UPPAAL (Invited Paper)

Kim Guldstrand Larsen

Department of Computer Science, Aalborg University, Denmark

In the talk we offer a detailed presentation on how the symbolic model checking techniques of Uppaal has joined forces with machine learning during the last 10 years.

The first step towards exploiting the efficiency of machine learning in UPPAAL was made in the branch UPPAAL SMC. Here [5], UPPAAL SMC offers highly efficient statistical model checking capabilities in order to provide performance analysis for a rich class of stochastic hybrid automata [10], and in a manner that consistently refines the Boolean verdicts of the model checking capability of classical UPPAAL. During the last 10 years this effort includes development of a sound theoretical foundation (e.g. the underlying stochastic semantics of timed automata [2]), the supporting algorithmic analysis (e.g. sequential testing a’la Wald), the efficient tool implementation as well as a long range of applications.

Most recently the SMC engine of UPPAAL has been considerably accelerated by exploiting independencies of system components during generation of random runs. In UPPAAL SMC, as in Gillespie’s algorithm for biochemical systems, components are repeatedly racing against each other, calling for a resampling of all components after each step. A challenge is to prove that resampling only step-dependent components leave the probability distribution on runs unchanged. Another challenge is to develop static analysis methods for identifying independencies. This in turn has significantly reduced the complexity of run-generation (from quadratic to – in practice – linear), allowing UPPAAL SMC to scale to millions of components, as witnessed by recent applications to so-called Agent-based models for COVID19 analysis with millions of components, e.g. one per citizen of Denmark [9]. In addition, using the SMC engine may be used to generate synthetic data from stochastic hybrid automata in order to learn Bayesian networks for inferring beliefs of key observable and unobservable properties in settings with scarce data [8].

In the most recent branch UPPAAL STRATEGO [4, 3], symbolic techniques are combined with reinforcement learning to efficiently obtain near-optimal yet safe strategies for hybrid Markov decision processes. Taking as inputs 1) a hybrid Markov decision process H , 2) a safe constraint ϕ and 3) an objective function O to be optimized, UPPAAL STRATEGO first provides a most permissive safety strategy guaranteeing that ϕ is fulfilled using a timed game abstraction of H . Here well-known symbolic model checking techniques are used. Next, applying various learning methods, sub-strategies (thus still safe) optimizing O are subsequently obtained. The talk will present new (Q-, M-, ...) learning methods developed [7], preliminary results on their convergence [6], the ability to learn and output small and explainable strategies using decision trees

[1], and the approach for taking partial observability into account. In addition the talk will provide a demonstration of the new UPPAAL STRATEGO on the Smart Farming Challenge of the Dagstuhl seminar “Analysis of Autonomous Mobile Collectives in Complex Physical Environments” (October 2019). Also on-going applications of UPPAAL STRATEGO on water-management, traffic-light control, energy-aware building ao will be pointed out.

During the next five-year period the effort on combining model checking and machine learning will continue in the newly granted Villum-Investigator Center S4OS¹ of the speaker.

References

1. Ashok, P., Křetínský, J., Larsen, K. G., Le Coënt, A., Taankvist, J. H., Weininger, M.: SOS: Safe, optimal and small strategies for hybrid markov decision processes. In: Parker, D., Wolf, V. (eds.) *Quantitative Evaluation of Systems. QEST 2019*. LNCS, vol. 11785, pp. 147–164 Springer, Cham (2019). https://doi.org/10.1007/978-3-030-30281-8_9
2. Bertrand, N., et al.: Stochastic timed automata. *Log. Methods Comput. Sci.*, **10**(4), 2014
3. David, A., et al.: On time with minimal expected cost!. In: Cassez, F., Raskin, J. F. (eds.) *Automated Technology for Verification and Analysis. ATVA 2014*. LNCS, vol. 8837, pp. 129–145. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11936-6_10
4. David, A., Jensen, P. G., Larsen, K. G., Mikučionis, M., Taankvist, J. H.: UPPAAL STRATEGO. In: Baier, C., Tinelli, C. (eds.) *Tools and Algorithms for the Construction and Analysis of Systems. TACAS 2015*. LNCS, vol. 9035, pp. 206–211. Springer, Berlin, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46681-0_16
5. David, A., Larsen, K. G., Legay, A., Mikucionis, M., Poulsen, D. B.: UPPAAL SMC tutorial. *Int. J. Softw. Tools Technol. Transf.* **17**(4), 397–415 (2015)
6. Jaeger, M., Bacci, G., Bacci, G., Larsen, K. G., Jensen, P. G.: Approximating euclidean by imprecise markov decision processes. In: Margaria, T., Steffen, B. (eds.) *Leveraging Applications of Formal Methods, Verification and Validation: Verification Principles. ISO LA 2020*. LNCS, vol. 12476, pp. 275–289. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-61362-4_15
7. Jaeger, M., Jensen, P. G., Guldstrand L. K., Legay, A., Sedwards, S., Taankvist, J. H.: Teaching stratego to play ball: optimal synthesis for continuous space MDPs. In: Chen, Y.F., Cheng, C. H., Esparza, J. (eds.) *Automated Technology for Verification and Analysis. ATVA 2019*. LNCS, vol. 11781, pp. 81–97. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-31784-3_5
8. Jaeger, M., Larsen, K. G., Tibo, A.: From statistical model checking to run-time monitoring using a bayesian network approach. In: Deshmukh, J., Ničković, D. (eds.) *Runtime Verification. RV 2020*. LNCS, vol. 12399, pp. 517–535. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-60508-7_30

¹ S4OS: Scalable analysis and Synthesis of Safe, Small, Secure and Optimal Strategies for CPS.

9. Jensen, P. G., Jørgensen, K. Y., Larsen, K. G., Mikučionis, M., Muñoz, M., Poulsen, D. B.: Fluid Model-Checking in UPPAAL for Covid-19. In: Margaria, T., Steffen, B. (eds.) *Leveraging Applications of Formal Methods, Verification and Validation: Verification Principles. ISoLA 2020*. LNCS, vol. 12476, pp. 385–403. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-61362-4_22
10. Larsen, K. G.: Statistical model checking, refinement checking, optimization, ... for stochastic hybrid systems. In: Jurdziński, M., Ničković, D. (eds.) *Formal Modeling and Analysis of Timed Systems. FORMATS 2012*. LNCS, vol. 7595, pp. 7–10. Springer, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-33365-1_2

Contents

Invited Papers

Concurrency and Objects Matter! Disentangling the Fabric of Real Operational Processes to Create Digital Twins.	3
<i>Wil M. P. van der Aalst</i>	
Qualitative–Quantitative Reasoning: Thinking Informally About Formal Things	18
<i>Alan Dix</i>	

Databases and Distributed Transactions

Some Aspects of the Database Resilience.	39
<i>Luis Henrique Bustamante and Ana Teresa Martins</i>	
On the Correctness Problem for Serializability	47
<i>Jürgen König and Heike Wehrheim</i>	

Efficient Model Checking Methods

A Set Automaton to Locate All Pattern Matches in a Term	67
<i>Rick Erkens and Jan Friso Groote</i>	
Accelerating SpMV Multiplication in Probabilistic Model Checkers Using GPUs.	86
<i>Muhammad Hannan Khan, Osman Hassan, and Shahid Khan</i>	
A Divide & Conquer Approach to Conditional Stable Model Checking	105
<i>Yati Phyoo, Canh Minh Do, and Kazuhiro Ogata</i>	

Formalization and Verification in Coq and Isabelle

Certifying Choreography Compilation	115
<i>Luís Cruz-Filipe, Fabrizio Montesi, and Marco Peressotti</i>	
A Mechanically Verified Theory of Contracts.	134
<i>Stéphane Kastenbaum, Benoît Boyer, and Jean-Pierre Talpin</i>	
A Complete Semantics of \mathbb{K} and Its Translation to Isabelle	152
<i>Liyi Li and Elsa L. Gunter</i>	

Quantum Computing

A New Connective in Natural Deduction, and Its Application to Quantum Computing	175
<i>Alejandro Díaz-Caro and Gilles Dowek</i>	

Security and Privacy

An Incentive Mechanism for Trading Personal Data in Data Markets.	197
<i>Sayan Biswas, Kangsoo Jung, and Catuscia Palamidessi</i>	
Assessing Security of Cryptocurrencies with Attack-Defense Trees: Proof of Concept and Future Directions	214
<i>Julia Eisentraut, Stephan Holzer, Katharina Klioba, Jan Křetínský, Lukas Pin, and Alexander Wagner</i>	
Compositional Analysis of Protocol Equivalence in the Applied π -Calculus Using Quasi-open Bisimilarity	235
<i>Ross Horne, Sjouke Mauw, and Semen Yurkov</i>	
Card-Based Cryptographic Protocols with a Standard Deck of Cards Using Private Operations.	256
<i>Yoshifumi Manabe and Hibiki Ono</i>	
Normalising Lustre Preserves Security	275
<i>Sanjiva Prasad and R. Madhukar Yerraguntla</i>	

Synthesis and Learning

Learning Probabilistic Automata Using Residuals	295
<i>Wenjing Chu, Shuo Chen, and Marcello Bonsangue</i>	
AICons: Deductive Synthesis of Sorting Algorithms in <i>Theorema</i>	314
<i>Isabela Drămnesc and Tudor Jebelean</i>	
Reactive Synthesis from Visibly Register Pushdown Automata	334
<i>Ryoma Senda, Yoshiaki Takata, and Hiroyuki Seki</i>	

Systems Calculi and Analysis

COMPLEXITYPARSER: An Automatic Tool for Certifying Poly-Time Complexity of Java Programs	357
<i>Emmanuel Hainry, Emmanuel Jeandel, Romain Péchoux, and Olivier Zeyen</i>	
A Calculus for Attribute-Based Memory Updates	366
<i>Marino Miculan and Michele Pasqua</i>	

A Proof Method for Local Sufficient Completeness of Term Rewriting Systems	386
<i>Tomoki Shiraishi, Kentaro Kikuchi, and Takahito Aoto</i>	
Author Index	405